

**IN THE UNITED STATES DISTRICT COURT  
FOR THE WESTERN DISTRICT OF WISCONSIN**

---

AUTHENTICOM, INC.

Plaintiff,

v.

CDK GLOBAL, LLC; and THE REYNOLDS  
AND REYNOLDS COMPANY

Defendants.

---

Civil Case No. 17-cv-318

**Declaration of Peter Swire**

**DECLARATION OF PETER SWIRE**

1. I have been asked to provide my expert opinion on issues relating to security and privacy for the actions of car dealerships and certain entities that do business with car dealerships.

2. My qualifications as a security and privacy expert are documented in a curriculum vitae, attached to this Declaration. In brief, I am the Huang Professor of Law and Ethics at the Georgia Tech Scheller College of Business, with appointments in the College of Computing and the School of Public Policy. I teach graduate and undergraduate courses in “Information Security Strategies and Policy” and “Privacy Technology, Policy, and Law.” From 1999 to 2001, I served as Chief Counselor for Privacy in the U.S. Office of Management and Budget and was the first person to have U.S. government-wide policy responsibility for privacy. In 2013, in the wake of the Snowden revelations, I was named one of five members of President Obama’s Review Group on Intelligence and Communications Technology. In 2015, among its more than 20,000 members, the International Association of Privacy Professionals awarded me its Privacy Leadership Award. I am Senior Counsel with Alston & Bird LLP.

3. This opinion addresses four main types of entities: (1) the providers of dealer management systems (“DMS”), notably CDK Global, LLC (“CDK”) and the Reynolds & Reynolds Company (“Reynolds”); (2) the car dealer (“Dealer”), whose data is entered into DMS and supplied to other entities; (3) the “Data Integrator,” including Authenticom and the data integration businesses of CDK and Reynolds; and (4) the third-party vendor (“Vendor”), which receives data from the Dealer, via a Data Integrator, and supplies applications or other services to the Dealer.

4. I have been asked to provide my expert opinion on the extent to which measures taken by CDK and Reynolds are reasonably necessary to protect the security and privacy of Dealer data.

5. My expert opinion, based on the facts available to me and my expertise in security and privacy, is that there is no security or privacy need that justifies CDK’s and Reynolds’ wholesale blocking of Authenticom and other independent Data Integrators from offering data integration services to Dealers and Vendors.

6. Part A of my Opinion explains that, for the relevant data, there is a strong historical basis for concluding that Dealers own the data and therefore have the right to grant data access to Data Integrators. Part B explains that Dealers have freely given affirmative, specific, and informed consent to supply data to Data Integrators and Vendors. Part C explains that all industries, including those with the most sensitive data such as personal health information, lawfully and extensively rely on third-party service providers, such as Data Integrators. Part D discusses the methods used by Data Integrators in the automobile Dealer sector and explains that the same methods are routinely used for more sensitive data in both the personal financial services and the

health sectors. The role that Data Integrators play in the personal financial services sector demonstrates that it is not reasonably necessary to preclude independent Data Integrators from serving Dealers and that independent Data Integrators like Authenticom can provide such services while maintaining security and privacy. Part E discusses additional facts that undermine any claim for a good-faith security concern, including that CDK and Reynolds themselves use Authenticom as a Data Integrator for their own applications. In conclusion, it is my opinion that there are no reasonable security and privacy concerns that justify CDK's and Reynolds' wholesale prohibition on the use of independent Data Integrators.

**A. The Dealers own the relevant data and have the right to grant access to Data Integrators.**

7. Based on documents supplied to me and statements from industry participants, including CDK and Reynolds, the clear historical record shows that the Dealers own the data made available to Data Integrators. The relevant data includes, but is not limited to:

- a) Customer information (*e.g.*, name, address, phone number, email address, and date of birth);
- b) Customer experience (*e.g.*, when a dealership contacted a customer, when the customer visited the dealership, and what cars the dealership showed him/her);
- c) Inventory (*e.g.*, cars and parts);
- d) Service information (*e.g.*, time of service appointments, cost of service to the Dealer, and profit earned on service); and
- e) Sales transactional information (*e.g.*, vehicle purchased, financing insurance, and trade-in information).

8. My understanding is that relevant parties have agreed and stated over time that the Dealer has a legal right to look at, use, and transfer such data for the Dealer's business purposes. For example, Tom Schwartz, Reynolds' chief spokesperson, publicly

declared: “The data belongs to the dealers. We all agree on that.”<sup>1</sup> On its website, Reynolds represents to dealers: “Your Data, Your Way. You own your data. Reynolds recognizes you need to share that data outside your dealership.”<sup>2</sup> Even Reynolds’ Customer Guide stated that “Reynolds acknowledges that your Business Data belongs to you,” while requiring Dealers to warrant that they “have all rights and authority to the Business Data.”<sup>3</sup>

9. Howard Gardner, CDK vice president over data strategy, has stated that CDK “has always understood that dealerships own their data and enjoy having choices on how best to share and utilize that data with others.”<sup>4</sup>

10. Steve Anenen, CDK’s longtime CEO, publicly stated: “I think we’ve stated pretty emphatically, we really believe the dealer owns the data. I don’t know how you can ever make the opinion that the data is yours to govern and to preclude others from having access to it, when in fact it’s really the data belonging to the dealer. As long as they grant permission, how would you ever go against that wish? I don’t understand that.”<sup>5</sup> CDK’s website states that “dealerships own their data,”<sup>6</sup> and CDK’s Master

---

<sup>1</sup> David Barkholz, *Dealers Decry Reynolds Crackdown*, Automotive News (Nov. 21, 2011), <http://www.autonews.com/article/20111121000100/RETAIL07/311219997?template=print>.

<sup>2</sup> Reynolds and Reynolds Company, *Fuel Ideas to Drive Performance*, <http://www.reyrey.com/dealernews/fuel/era/2010/vol1/Your-Data-Your-Way.asp>.

<sup>3</sup> Reynolds and Reynolds Company, *Customer Guide* at 8, Version 8 (Jan. 1, 2009); *see also id.* at 9 (acknowledging that Business Data includes customer personal financial information).

<sup>4</sup> ADP Dealer Services, Inc., Press Release, *ADP Announces New Approved Vendors for ADP’s Third Party Access Program* (July 12, 2013), [http://www.reactornet.com/company/news/12/reactornet\\_adp\\_integration](http://www.reactornet.com/company/news/12/reactornet_adp_integration).

<sup>5</sup> Ralph Kisiel, *ADP Provides Dealers 3 Options on Data Access*, Automotive News (Feb. 19, 2007) (quoting CDK president Steve Anenen), <http://www.autonews.com/article/20070219/SUB/70215040/adp-provides-dealers-3-options-on-data-access>.

Services Agreement states that “[a]ny Client file or other information provided by Client to CDK for use with the Services . . . shall remain the exclusive and confidential property of Client.”<sup>7</sup>

11. I understand that the Dealers themselves, industry organizations (including the National Auto Dealers Association (“NADA”)), and Vendors have likewise taken the same position. In February 2007, for example, the National Auto Dealers Association and the American International Automobile Dealer Association issued a “Joint Policy Statement on Data Accessibility,” which included the statement that “[d]ealers should control access to the data stored in their dealership management systems.”<sup>8</sup>

12. I understand that first Reynolds, and more recently CDK, have changed positions and now block Dealers under their contracts from granting independent Data Integrators access to the Dealer data.

**B. Dealers have freely given affirmative, specific, and informed consent to transfer data to Data Integrators and Vendors.**

13. I have reviewed contracts between (1) Dealers and Authenticom; and (2) Authenticom and Vendors. Under these contracts, data is transferred from Dealers to Authenticom, on the understanding that the data will then be transferred to Vendors. From my experience in numerous privacy and cybersecurity regimes, the gold standard

---

<sup>6</sup> CDK Global, *Third Party Access Program: What Dealers Need to Know*, [http://www.cdkglobal.com/sites/default/files/Third\\_Party\\_Access\\_Program\\_Solution\\_Overview\\_%28What\\_Dealers\\_Need\\_to\\_Know%29.pdf](http://www.cdkglobal.com/sites/default/files/Third_Party_Access_Program_Solution_Overview_%28What_Dealers_Need_to_Know%29.pdf).

<sup>7</sup> CDK Master Services Agreement § 7.A.

<sup>8</sup> See NADA, Press Release, *NADA, AIADA Issue Joint Policy Statement on Data Accessibility* (Feb. 2, 2007), <https://www.nada.org/CustomTemplates/DetailPressRelease.aspx?id=21474842320>.

for assessing consent is to demonstrate that the consent is freely given, affirmative, specific, and informed.<sup>9</sup> That gold standard is met in these contracts:

- a) **Freely given consent.** Dealers that contract with Authenticom are doing so freely. The Dealers have other choices in the market, including the Data Integrator businesses of the large companies CDK and Reynolds. In the presence of such choices, many Dealers have chosen Authenticom.
- b) **Affirmative consent.** Dealers affirmatively opt-in to the data relationship with Authenticom. In many settings relevant to privacy and security, there has been a debate about whether the individual in control of the information should be provided an “opt-in” or “opt-out” choice. “Opt-in” regimes are stricter, as they require affirmative action. For “opt-out” regimes, the default is that data is shared, unless the individual objects. For the relationship between Dealers and Authenticom, the stricter standard is used – i.e., an affirmative decision by the Dealer to opt-in to the data being shared.
- c) **Specific and informed consent.** The Dealers provide data to DealerVault pursuant to detailed Terms and Conditions, which explain in considerable detail how data will be transferred. The Terms and Conditions also provide information on Authenticom’s data security and privacy practices. In addition to these contractual terms, Dealers engage Authenticom precisely for the purpose of transferring data to Vendors. Accordingly, Dealers that hire Authenticom provide informed consent.

---

<sup>9</sup> Affirmative (opt-in) consent is required, for instance, under the HIPAA Medical Privacy Rule and other strict regimes, such as the Wiretap Act, governing whether an individual has consented to interception of communications. *See* 18 U.S.C. § 2511. An even more detailed consent regime applies in the European Union, which has data protection laws for the commercial sector that are considered stricter than under U.S. law. *See* Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995 O.J. (L 281) 31, Art. 2(h) (defining an individual’s consent as “any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed”), *available at* [http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46\\_part1\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf); Article 29 Data Protection Working Party, *Opinion 15/2011 on the definition of consent*, 01197/11/EN WP187, § III.A.4 (July 13, 2011) (stating unambiguous consent “is more likely to be obtained when individuals engage in an affirmative action to signify their agreement”), *available at* [http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf). The point in text is that the consent provided by Dealers is strong enough to meet the standards for medical privacy and wiretaps in the United States, and the notably strict privacy regime in the European Union.

14. This high standard for consent is relevant to the point, discussed above, that “it is the Dealer’s data.” Part A established that the Dealers own the data and have strong rights to grant access to the data. Part B establishes that the Dealers, possessed of those strong rights, have properly consented to the data being transferred to the Data Integrator, and then to Vendors.

**C. All industries, including those with the most sensitive data, lawfully rely extensively on third party service providers.**

15. It is my understanding that CDK and Reynolds have asserted that the mere existence of an intermediary Data Integrator creates a security risk that justifies blocking all independent Data Integrators like Authenticom from having any access to Dealer data. For example, Bob Karp, President of CDK North America, wrote in an August 22, 2016 letter to Dealers that it was “necessary” to eliminate “use of intermediaries” other than those affiliated with CDK. He asserted that use of non-CDK-affiliated intermediaries inherently created “unacceptable levels of security risk” because, when data moves from a Dealer to a Vendor, it

must move through one or more data-handling intermediaries before it is received by the [Vendor]. Each separate data transmission and stop over point increases the risk of loss, misdirection, and/or misuse of dealership data.<sup>10</sup>

16. Based on my experience in many industry sectors, it is my opinion that the presence of “data-handling intermediaries” is pervasive and well-accepted. Moreover, data can and does pass through such intermediaries consistent with privacy and security requirements.

---

<sup>10</sup> Letter from Bob Karp to Dealers (Aug. 22, 2016).

17. I became particularly familiar with the role of such intermediaries when I was the White House coordinator for the HIPAA Medical Privacy Rule, for the proposed rule issued in 1999, through the response to more than 50,000 public comments, and in the final rule issued in 2000. I highlight two features of the HIPAA Medical Privacy Rule to show the importance of such intermediaries. First, the HIPAA Medical Privacy Rule defines covered entities to include health plans, health providers, and health care clearinghouses.<sup>11</sup> Health care clearinghouses are the relevant category here. Their main function is to act as intermediaries for health care billing records. A health care provider, such as a physician practice group, sends its records to the clearinghouse, which performs functions similar to those of a Data Integrator – the clearinghouse cleanses the data, puts the data into standard formats, and then transmits the cleansed data to the entity that will pay the bill. In short, for sensitive health care billing information – which might, for example, state the procedures or tests a patient has undergone or the medications that patient takes – the HIPAA Medical Privacy Rule explicitly accepts the lawfulness and need for clearinghouses to serve this data integration, intermediary function.

18. Second, the HIPAA Medical Privacy Rule authorizes the use of “business associates.”<sup>12</sup> The Rule recognizes that many data processing and other functions are not provided by the health care provider, whose core competence is health care delivery. Instead, health care providers often rely on third parties, called “business associates,” to provide data processing and other services. These intermediaries have access to and process confidential health care information. By authorizing the use of such business associates, the HIPAA Medical Privacy Rule explicitly accepts the lawfulness and need

---

<sup>11</sup> See 45 C.F.R. § 160.103.

<sup>12</sup> See 45 C.F.R. § 164.502(e)(1)(i).



for health care providers to rely on outside parties for data integration and processing functions.

19. In my opinion, these HIPAA examples demonstrate that the use of data intermediaries is consistent with maintaining privacy and security, and therefore that privacy and security cannot justify a per se prohibition on the use of Data Integrators. Data integration is used on a widespread basis in the health care sector, which is heavily regulated and involves very sensitive personal information. Moreover, the type of information that is available to Data Integrators in the car dealer market – like customer names and contact information and the other data commonly sent to Data Integrators – is typically much less sensitive than health information. In my opinion, the wholesale blocking of Data Integrators undertaken by CDK and by Reynolds is not reasonably necessary to protect the security and privacy of Dealer data.

**D. The methods used by Data Integrators in the car dealer sector are routinely used for more sensitive data in the personal financial services sector.**

20. The security methods used by Data Integrators in the car dealer sector are routinely used for considerably more sensitive data in the personal financial services sector. In both the car dealer and financial services markets, Data Integrators use login credentials provided by the owner of the data in order to gain access to the data. Moreover, there appears to be a history of effective data protection in both the car dealer and banking sectors. The history and practice in the financial services sector thus provides an additional basis for concluding that per se limits on data access advocated by CDK and Reynolds are not reasonably necessary to the actual protection of security and privacy.

**21.** In November 2016, the Consumer Financial Protection Board (“CFPB”) issued a notice and request for information concerning “consumer rights to access financial account and account-related data in usable electronic form.”<sup>13</sup> For consumer financial services, companies such as Intuit, Plaid, and Yodlee receive permission and login credentials from consumers and then access multiple accounts held by the consumer, in order to offer consolidated financial statements and a variety of other consumer services. Some banks have objected to this consumer-provisioned access to Data Integrators such as Intuit, arguing that the existing methods of access were insufficiently secure. This is parallel to how CDK and Reynolds have objected to Dealer-approved access to Data Integrators such as DealerVault.<sup>14</sup>

**22.** In the notice, the CFPB expressed concern “that some market participants may decide to restrict consumer-permissioned access to data in ways that undermine consumer interests . . . and that are broader than necessary to address legitimate privacy and security concerns.”<sup>15</sup> These concerns precisely track the concerns of Dealers who may lose access to competitive services such as Authenticom. The concerns, for both

---

<sup>13</sup> Notice and Request for Information, Request for Information Regarding Consumer Access to Financial Records, 81 Fed. Reg. 83,806, 83,806 (Nov. 22, 2016).

<sup>14</sup> An important difference is that the financial services sector contains thousands of institutions. Commercial banking and other financial services integrated with services such as Intuit do not feature the very high market concentration that I understand to be held by CDK and Reynolds.

In addition, banks have a financial incentive to be concerned about fraudulent logins that is greater than for CDK and Reynolds; in many instances, banks take the loss for unauthorized use of credit cards, debit cards, and checking accounts, so that the banks have substantial financial exposure based on mistaken transactions. By contrast, CDK and Reynolds have no financial risk of similar magnitude if the Dealers use a screen-scraping servicing, and so CDK and Reynolds have less of a risk-based basis than banks for blocking user-authorized access.

<sup>15</sup> 81 Fed. Reg. 83,809.

consumers and Dealers, are that their access to services may be restricted even though “no aggregator has been the victim of a known major data breach” for financial services,<sup>16</sup> and there is similarly no public history of a breach by Data Integrators for the car dealer industry.<sup>17</sup> This lack of known instances of breach is consistent with an overall view of low risk of security problems due to the intermediary role played by Data Integrators in the auto dealer industry.

**23.** Based on my experience and expertise in data privacy and security, it is my opinion that Data Integrators pose dramatically less security and privacy risk in the car dealer sector than the consumer financial sector, for at least three reasons:

- a) The contract between car Dealers and Data Integrators is a business-to-business (B2B) contract, in contrast to the business-to-consumer (B2C) contracts for financial services. For B2B contracts, the business ordering the service – the Dealer – is presumed to be in the best position to assess the risks and benefits of the contract. Given the business sophistication of the Dealer, as well as the Dealer’s freely given, affirmative, specific, and informed consent, there is no logical basis for a provider of DMS to override the Dealer’s own judgment about the risks and benefits of alternative data practices. By contrast, consumer protection laws are far stricter for B2C contracts, especially in the financial services area where consumers have often been preyed upon by fraudsters. Thus, the B2B nature of the contract between the Dealer and Data Integrator means that there is far less basis for a paternalistic rule against Data Integration in the auto dealer industry than for consumer financial services.
- b) The consumer financial services contracts are notably high risk. If a Data Integrator acts in a negligent or malicious way, the consumer’s entire banking or other account could be drained. The same level of financial risk does not exist for the data at issue in this case. As a related point, the incentive for attackers to go after a consumer’s entire bank account is far greater than for an attacker to target Dealer data.

---

<sup>16</sup> Robin Sidel, *Big Banks Lock Horns With Personal-Finance Web Portals*, Wall St. J. (Nov. 4, 2015), <https://www.wsj.com/articles/big-banks-lock-horns-with-personal-finance-web-portals-1446683450>.

<sup>17</sup> I understand that there is one reported incident where an employee of a Vendor, eLeads, improperly accessed data in that Vendor’s database, but that incident had nothing to do with the use of Data Integrators. I am not aware of any data breach related to the activities of a Data Integrator in the car dealer industry.

- c) As the CFPB explains, there are thousands of Data Integrators and Vendors in the consumer financial sector. By contrast, the number of Data Integrators and Vendors in the car dealer sector is much smaller. This means that it is far more manageable to assess the security and privacy issues for each Dealer contract with a Data Integrator or Vendor, allowing tailored means for assuring security and privacy if necessary.

**24.** While the CFPB has expressed awareness of the possible security concerns with the practices of financial Data Integrators, the statements of the CFPB support the conclusion that it has issued its Request for Information primarily to protect the interests of consumers against overly restrictive bank practices concerning the consumers' own data.

**25.** In my opinion, the case for concern about excessive restrictions, not justified by security, is far greater for Dealers. The data held by Dealers has far lower security risks than the data held by banks and lacks the risk of stealing from bank accounts. For B2B contracts, such as those that Dealers make with DealerVault, the presumption of validity is stronger than for contracts subject to consumer protection. The ability of Dealers to fine-tune their own contracts is also far greater in the auto industry than for the far higher number of participants in financial services. For all of these reasons, if the restrictions sought by banks appear unnecessary and too restrictive, the restrictions sought by CDK and Reynolds deserve much greater suspicion.

**E. Additional facts do not fit well with the claimed security concerns.**

**26.** Based on documents supplied to me and my understanding of the procedures used by Authenticom, there are other facts that do not fit well with the stated security concerns claimed by CDK and Reynolds. For the following six items, the facts available to me support an inference that CDK and Reynolds are not making a valid

security argument when they exclude Dealers from using data integration services with Authenticom.

**27.** First, I have reviewed the technical mechanisms used by Authenticom to pull data from Dealers' DMS databases. Essentially, Authenticom uses the same mechanism to access data from the DMS as a Dealer employee does. Contrary to implications made by Defendants,<sup>18</sup> the Authenticom process does not put any code onto the DMS; for both employee and Authenticom access, a user authorized by the Dealer makes the request to retrieve data, with the difference being that Authenticom automates the process whereas the Dealer employee retrieves the data manually.

**28.** Second, CDK apparently has Data Integrators in its corporate family that use the same techniques as Authenticom. CDK's subsidiaries Digital Motorworks and IntegraLink perform data integration services for Dealers. My understanding is that Digital Motorworks and IntegraLink use login credentials provided by the Dealers. If this approach is secure enough for Digital Motorworks and IntegraLink – i.e., CDK – then security would not seem to be a basis for excluding Authenticom.

**29.** Third, I understand that Reynolds itself uses Authenticom to supply data integration services in some instances. Reynolds uses Authenticom to pull data from some Reynolds dealers for data integration with Reynolds' own applications. This use of Authenticom supports the inference that Authenticom provides a useful service for Dealers and that the security techniques used by Authenticom are sufficient for Reynolds.

**30.** Fourth, I understand that Reynolds and CDK similarly use Authenticom in connection with their wholly owned joint venture, AVRS, Inc. That company provides

---

<sup>18</sup> Letter from Bob Karp to Dealers (Aug. 22, 2016).

electronic vehicle registration and titling services for Dealers in California. It is my understanding that AVRS uses Authenticom for data integration services, so that Authenticom pulls data from CDK and Reynolds Dealers and provides that data to AVRS. Once again, this practice by the CDK/Reynolds joint venture supports the view that the security techniques used by Authenticom are sufficient to secure Dealer data.

**31.** Fifth, the practices of CDK before it entered into a “Wind Down Access” Agreement with Reynolds in February 2015 support the inference that Authenticom is being blocked for reasons other than security. Until February 2015 – and for a year or more thereafter during the “wind down” period – it is my understanding that CDK itself provided data integration services for Reynolds Dealers by obtaining login credentials from those dealers. In other words, the business model and techniques used by Authenticom, to service Dealers, were also used by CDK to service Reynolds dealers until the February 2015 agreement. I am not aware of anything that changed in February 2015 that suddenly rendered those techniques insufficient to protect Dealer data.

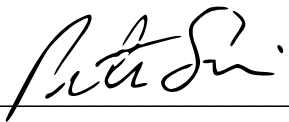
**32.** Sixth and finally, there is considerable evidence that Authenticom uses strong security practices. Based on the information available to me, the company has never had a data breach. It uses secure encryption technology to transmit data and has received a Microsoft gold certification for the past three years. Moreover, Authenticom has at least \$15 million cyber security insurance policy to indemnify Dealers in case of a security problem, although no such need has ever arisen. As stated above, the type of data held by Dealers is generally considerably less sensitive than health or financial data, so \$15 million of insurance would appear to be ample for any realistic risks from any eventual problem with Authenticom’s security. Because Dealers thus seem highly likely

to be held harmless in the event of a security problem, security risks would appear to be a very weak basis for preventing Dealers from contracting with Authenticom.

### **CONCLUSION**

**33.** It is my opinion that there is no reasonable security and privacy need that justifies the wholesale efforts by CDK and Reynolds to exclude Authenticom from the role of Data Integrator for dealers using the CDK and Reynolds dealer management software. Authenticom appears to use standard and accepted techniques for transferring data. The types of data transferred to Data Integrators are considerably less sensitive than those used in the medical record and financial services context, yet similar data integration and other software service provision commonly exist in those sectors. Moreover, the practices used by Authenticom (and CDK's own subsidiaries, Digital Motorworks and IntegraLink) are substantially similar to the practices used by Data Integrators in the health care and financial industries when dealing with even more sensitive information. If those practices are sufficient to protect the more sensitive information at risk in the financial services and health care industries, it is my opinion that those practices are sufficient to address privacy and security concerns in the integration market for Dealer data. Dealers apparently agree, as they used (and continue to use) third-party integrators like Authenticom before Reynolds and CDK tried to block them from doing so. Accordingly, it is my opinion that the wholesale blocking of Data Integrators is not reasonably necessary and that independent Data Integrators like Authenticom can provide data integration services while maintaining security and privacy.

Dated: May 17, 2017

By:   
Peter P. Swire